I Smell a Rat!

A Digital Forensics Approach

Cristian Coraci
The Open University

November 2019
Session FL

Disclaimer

- All data shown during demos are fictitious
- Any similarities with actual persons are only coincidental
- Do not try to use bank or personal details; they are randomly generated and not real

What is Digital Forensics and where is it used?

- A branch of forensic science that is used to recover and investigate material found in digital devices (e.g. computers, mobiles, PDAs, smartwatches, Memory cards, USB flash drives, Hard disk drives, etc.)

- It is commonly associated with e-crime, such as child pornography or credit card fraud
- Nowadays it is used to prosecute all kind of crimes, not only e-crimes
- It can also be used in prevention of major data leaks of Intellectual Property (IP)

I smell a rat! How do they transmit data outside?

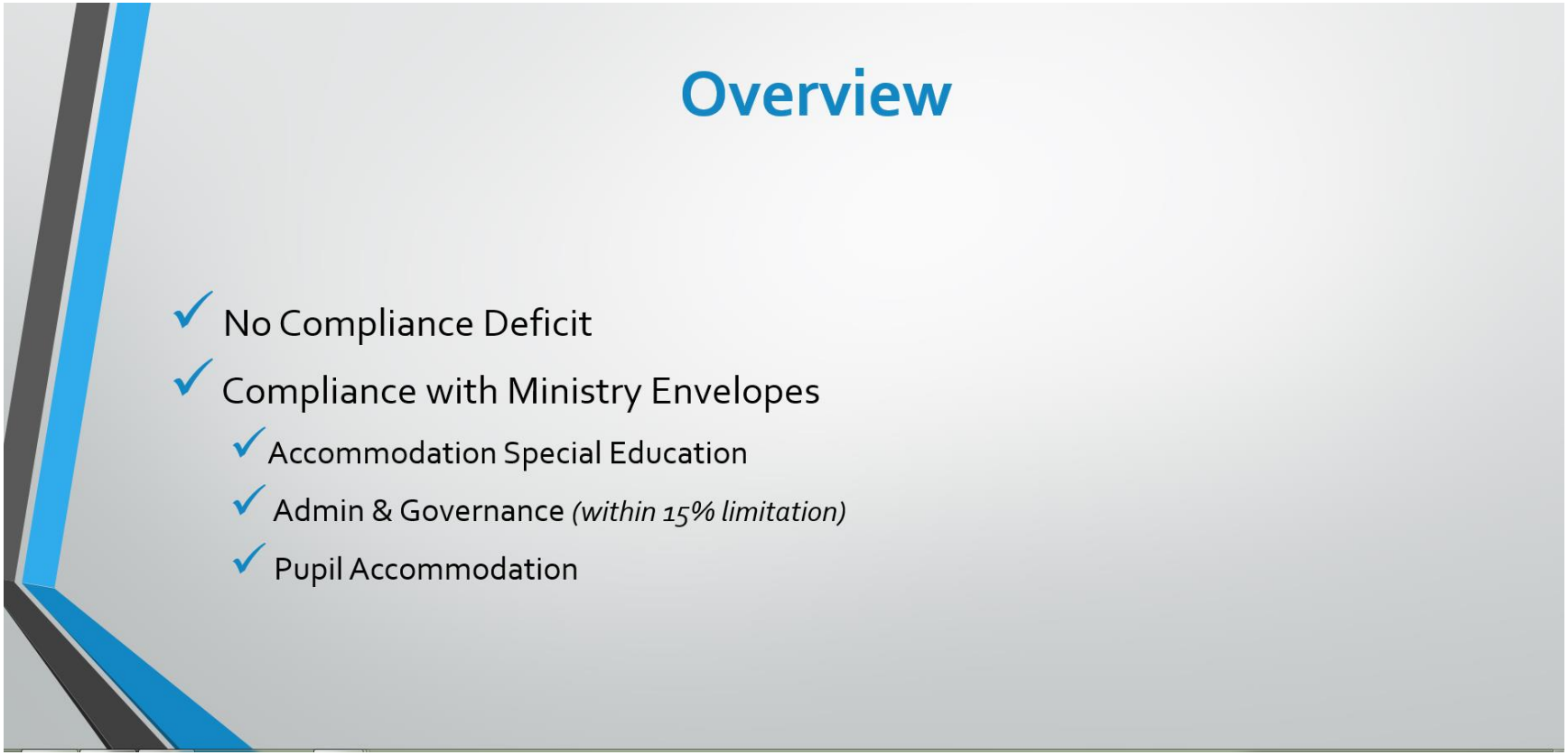
Insiders can be:

- Whistle-blowers (Edward Snowden)
- Disgruntled employee (Martin Tripp/Tesla)
- Any employee leaving (or not) the job

There are various possibilities to transmit data outside without that being obvious, from basic techniques such as base64 encryption, to much more complex methods, like file embedding, photograph geo-tagging, annotations, etc.

Hiding Notes in PowerPoint Slides

A really childish method, but sometimes very effective



In full-screen mode there is no visible information

Hiding Notes in PowerPoint Slides

But when entering edit (design) mode the note becomes visible.

Base64 Encoding

- A very effective method of transmitting small amounts of data using an .htm, .html or .xml file
- Inside such a file one can embed base64 encoded information without affecting the functionality of the page
- The encrypted content is shown by <base64> delimiters and looks like normal HTML encoding for the untrained eye

File renaming (extension changing)

- Changing the file extension in order to trick the operating system and the user
- The file type is changed and the operating system will use the appropriate program to read it
- Effective method for leaking photographs and other types of images

Photograph geo-tagging

- This method is used to leak information about classified locations
- The geo-location information are not erased from file's details, therefore allowing precise pinpointing
- Having these details one can use Google Maps or other service to find out where that photograph has been taken
- Needs specialised applications

Quoted/Printable Encoding

- A much more dangerous method that is used to leak large chunks of data using apparently ordinary emails
- Most of the email applications are displaying the header and body only, ignoring the rest of the content
- Inside the body one can embed large amounts of data by using the quoted/printable encryption method
- The data will not affect the way the email is displayed
- But if one is asking the email client to display the source all this hidden content becomes visible

Steganography

- A technique of hiding secret data within an ordinary image in order to avoid detection
- The word is derived from Greek words “steganos” meaning “covered, concealed, or protected” and “graphein” meaning “writing”

File embedding

- A very dangerous method that allows one to leak huge amounts of data in apparently inoffensive files
- The technique consists of embedding an archive into a photograph
- The resulting file is shown as image and can be opened with any image viewer without giving away the hidden content
- Requires advanced knowledge about properties of different file types

Thank you

Please submit your session feedback!

- Do it online at http://conferences.gse.org.uk/2019/feedback/fl
- This session is FL